UNITED STATES OF AMERICA	)	
	)	
v.	)	**Prosecution Response**
	)	
Manning, Bradley E.	)	**to Defense Motion to**
PFC, U.S. Army,	)	**Compel Discovery**
HHC, U.S. Army Garrison,	)	
Joint Base Myer-Henderson Hall	)	**8 March 2012**
Fort Myer, Virginia 22211	)	

RELIEF SOUGHT

The United States respectfully requests the Court deny, in part, the Defense Motion to Compel Discovery (hereinafter "Defense Motion") for the reasons provided herein. The United States requests oral argument.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the Defense bears the burden of persuasion and must prove any factual issues necessary to decide this motion by a preponderance of the evidence. See Manual for Courts-Martial, United States, R.C.M. 905(c) (2008).

FACTS

The United States stipulates to those facts cited in Defense Motion, except for any allegations that are inconsistent with the following:

The Department of Defense Directives cited by Defense in paragraph 5(a) only apply to the compromise of Sensitive Compartmented Information, which the United States has no reason to believe occurred.

The United States disputes any allegation, including those relating to whether, when, and to what extent select agencies, departments and organizations reviewed the compromised information, supported by unofficial public statements.

The United States took all necessary measures and precautions to ensure Defense received efficient, yet accurate, discovery responses. The United States produced discoverable information as immediate as possible to avoid any further delay, upon receipt of the appropriate approvals for classified information, if applicable.

On 16 November 2011, Defense did not specifically request files completed with the assistance of the Office of the Director of National Intelligence. See Enclosure 4.

The Defense provides no evidence to support its proposition that an inspection of any computers "would have allowed the Defense to provide evidence that it was common for [S]oldiers to add technically unauthorized computer programs to their computers."

On 1 December 2011, the Defense did not specifically request any alleged information completed by the WikiLeaks Task Force (WTF). See Enclosure 5.

The Defense provides no evidence to support its proposition relating to what the Information Review Task Force (IRTF) concluded and from whom, if anyone, the Department of Defense (DOD) sought assistance.

The Defense provides no evidence to support its proposition relating to what, if anything, the alleged Department of State (DOS) task force concluded and that any alleged conclusions were "at odds with the classification review."

The United States disputes that the Article 32 Investigating Officer (IO) should have ordered production of evidence. The United States concurs with the IO's determination.

On 3 October 2011, the United States produced all enclosures to any Freedom of Information Act (FOIA) response, specifically BATES 00000772-00000851. See Enclosure 7.

Upon Defense request, the United States promptly preserved all Quantico videos requested by Defense. See Enclosure 1. On 6 December 2011, the United States produced all videos of the alleged Quantico incident, specifically BATES 00408902-00408903. See Enclosures 1-3 and 8. The alleged video referenced by the Defense does not exist. See id.

On 21 September 2011 – more than one year after the accused's unit redeployed back to Fort Drum, New York – the Defense requested that the United States preserve these hard drives. See Enclosure 9. The United States identified four commands or agencies that may possess hard drives responsive to this request and promptly submitted a Request to Locate and Preserve Evidence to each command or agency. Those entities included: (1) 2d Brigade Combat Team, 10th Mountain Division (2/10 MTN); (2) the Federal Bureau of Investigation (FBI); (3) Third Army, United States Army Central (ARCENT); and (4) the Computer Crime Investigative Unit, U.S. Army Criminal Investigative Command (CCIU). See Enclosures 10-13.

The United States' request to 2/10 MTN yielded the preservation of 181 hard drives, of which the United States has identified thirteen as being located within the SCIF during the unit's deployment to FOB Hammer. See Enclosures 15-16. None of those thirteen hard drives contained the "bradley.manning" user profile. See id.

The ARCENT Commander confirmed that the "command does not have possession of any Theater Provided Equipment hard drives responsive to [the United States'] request," which would account for any equipment which did not redeploy with the unit. Enclosure 17. Similarly, the FBI confirmed it has no hard drives responsive to the United States' request, outside those collected by Army Criminal Investigation Command (CID).

On 30 May 2010 and while at FOB Hammer, Iraq, CID recovered three hard drives from the SCIF, including both Secret Internet Protocol Router Network (SIPRNET) computers assigned to the accused and the Non-Secure Internet Protocol Router Network (NIPRNET) computer assigned to SFC Adkins, the accused's Noncommissioned Officer-in-Charge. See

Enclosures 18-19. Only the two hard drives assigned to the accused contained the "bradley.manning" user profile. See id. On 8 November 2011, the United States produced an EnCase forensic image of all three hard drives, including both containing the "bradley.manning" user profile. See Enclosure 20; see also Enclosure 32 (Voucher 073-10).

On 10 September 2010 and while at Fort Drum, New York, CCIU searched the Shipping Containers (hereinafter "CONEX") from the accused's unit. See Enclosure 16. CCIU identified ninety-one hard drives that were located in the SCIF during the accused's deployment. See id. Only one hard drive contained the accused's user profile. See id. On 16 September 2010, CCIU examined this hard drive and discovered that the computer was "utilized by the assigned user "bradley.manning" between 08:47:15, 04 Jun 09 and 14:20:00, 24 Sep 09." Enclosure 22. The hard drive did not contain the accused's user profile during the accused's deployment. See id.; see also Enclosure 23. On 8 November 2011, the United States produced an EnCase forensic image of this hard drive. See Enclosure 20; see also Enclosure 32 (Voucher 132-10).

On 30 September 2010, CCIU requested that 2/10 MTN preserve "any additional hard drives used during the deployment to Iraq." Enclosure 24. On 1 October 2010, pursuant to a search authorization, CCIU searched "the remaining drives in the 2/10 MTN SCIF." Enclosure 25. CCIU identified thirty-three hard drives that were located in the SCIF during the accused deployment. See id. Only two hard drives contained the accused's user profile. See id.; see also Enclosure 26. On 4 October 2010, CCIU created an EnCase forensic image of these hard drives. See id. On 8 November 2011, the United States produced the EnCase forensic images of both hard drives containing the accused's user profile. See Enclosure 20; see also Enclosure 32 (Voucher 147-10).

To date, the United States has produced 2,686 unclassified documents, totaling 80,026 pages, and 41,200 classified documents, totaling 331,340 pages, to the Defense. In sum, the United States has produced a total of 43,886 documents, consisting of 411,366 pages. See Enclosure 28 (most recent production of sequential discovery).[1]

WITNESSES/EVIDENCE

The United States does not request any witnesses be produced for this response. The United States respectfully requests that the Court consider the following enclosures to this response:

1. Request for Prudential Search and Preservation of Information to Quantico, 28 April 2011
2. Response to Preservation Request from Lieutenant Colonel (LtCol) Chris Greer, United States Marine Corps of Quantico, 20 December 2011
3. Sworn Statement, Master Sergeant (MSgt) Brian Papakie, United States Marine Corps

[1] For a detailed explanation of the number of classification authorities involved and the procedure/time necessary for approval for production or alternatives under MRE 505, see Prosecution Supplement to Prosecution Proposed Case Calendar, dated 8 March 2012.

4. Defense Discovery Request, 16 November 2011
5. Defense Discovery Request, 1 December 2011
6. Prosecution Discovery Response, 31 January 2012
7. Delivery confirmation (BATES 00000001-00044864)
8. Delivery confirmation (BATES 00408202-00409678)
9. Defense Preservation Request, 21 September 2011
10. Prosecution Preservation Request (2/10 MTN), 04 October 2011
11. Prosecution Preservation Request (FBI), 04 October 2011
12. Prosecution Preservation Request (ARCENT), 06 October 2011
13. Prosecution Preservation Request (CCIU), 04 October 2011
14. Sworn Statement, MAJ Latendresse, 06 March 2012
15. Preservation List, 2/10 MTN
16. Agent's Investigation Report, SA Wilbur (BATES 00021963)
17. ARCENT response to Preservation Request, 20 October 2011
18. DA Form 4137 (BATES 00411038)
19. DA Form 4137 (BATES 00411040)
20. Delivery Confirmation, dated 8 November 2011
21. DA Form 4137 (BATES 00411124)
22. Agent's Investigation Report, SA Shaver, 17 September 2010 (BATES 00022379)
23. Enlisted Record Brief, PFC Bradley Manning, 20 January 2012 (BATES 00410877)
24. Preservation Request, CID, 30 September 2010 (BATES 00024504)
25. Agent's Investigation Report, SA Ellis, 01 October 2010 (BATES 00022135)
26. Agent's Investigation Report, SA Shaver, 4 October 2010 (BATES 00022422)
27. DA Form 4137 (BATES 00411147)
28. Delivery Confirmation, 27 January 2012
29. Defense Discovery Request, 13 October 2011
30. Defense Discovery Request, 8 December 2010
31. Defense Discovery Request, 13 May 2011
32. Images on Cube[2]

LEGAL AUTHORITY AND ARGUMENT

The United States respectfully request the Court deny Defense request to compel the production of the following: (1) internal discussion of any FOIA request; (2) EnCase forensic images of all preserved hard drives that do not contain the "bradley.manning" user profile; (3) and damage assessments and records from the Central Intelligence Agency (CIA), Department of Defense (DOD) (including all agencies or departments referenced in Defense Motion, para. 1(d)(2)), Department of Justice (DOJ), and Department of State (DOS).

[2] On 8 November 2011, the United States produced a "Cube" to the Defense. Enclosure 32 lists those items contained on the "Cube."

I: THE UNITED STATES BEARS AN OBLIGATION TO PRODUCE UNCLASSIFIED DISCOVERY PURSUANT TO THE RULES FOR COURTS-MARTIAL AND THE CONSTITUTION OF THE UNITED STATES.

Rule for Courts-Martial (R.C.M.) 703(f) and the Supreme Court ruling in Brady outline the obligation of the United States to produce unclassified discovery. See R.C.M. 703(f); see also Brady v. Maryland, 373 U.S. 83 (1963).

A. Rule for Courts-Martial 703(f) requires the United States to produce unclassified information that is "relevant and necessary."

RCM 703(f) states that "[e]ach party is entitled to the production of evidence which is relevant and necessary." R.C.M. 703(f)(1); see also R.C.M. 401 (relevant evidence "means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence"); see also R.C.M. 703(f)(1), Discussion ("[r]elevant evidence is necessary when it is not cumulative and when it would contribute to a party's presentation of the case in some positive way on a matter in issue"). The rule continues that "any defense request for the production of evidence shall list the items of evidence to be produced and shall include a description of each item sufficient to show its relevance and necessity." See R.C.M. 703(f)(3); see also Pennsylvania v. Ritchie, 480 U.S. 39, 59 (1987) (the accused "has no constitutional right to conduct his own search of the [government's] files to argue relevance").

The rule continues that "a party is not entitled to the production of evidence which is destroyed, lost, or otherwise not subject to compulsory process." R.C.M. 703(f)(2) (only "if such evidence is of such central importance to an issue that it is essential to a fair trial, and if there is no adequate substitute for such evidence, the military judge shall grant a continuance or other relief in order to attempt to produce the evidence"); see also United States v. Ellis, 57 M.J. 375 (C.A.A.F. 2002) (the inquiry hinges of whether the evidence is of "central importance to an issue" absent adequate substitute).

The rule does not govern the production of classified information. See R.C.M. 701(f) ("nothing in this rule shall…require the disclosure of information protected from disclosure by [MRE 505]"); see also R.C.M. 703(f) analysis; see also Manual for Courts-Martial, United States, Mil. R. Evid. 505(a) ("this rule applies to all stages of the proceedings").

B. The Supreme Court ruling in Brady imposes a constitutional duty upon the United States to produce any favorable evidence that is material to guilt or punishment.

The prosecution shall disclose evidence that is favorable to an accused and that is material either to guilt or punishment. See Brady, 373 U.S. at 83. Favorable evidence includes exculpatory and impeachment evidence. See id. at 83; see also Giglio v. United States, 405 U.S. 150, 154 (1972). Favorable evidence "is subject to constitutionally mandated disclosure when it 'could reasonably be taken to put the whole case in such a different light as to undermine confidence in the verdict.'" Cone v. Bell, 556 U.S. 449, 464 (2009) (citing Kyles v. Whitley, 514 U.S. 419, 435 (1995)). Evidence "is 'material' within the meaning of Brady when there is a

reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different." Cone, 556 U.S. at 469 ("[e]vidence that is material to guilt will often be material for sentencing purposes as well; the converse is not always true"); see also United States v. Agurs, 427 U.S. 97, 112 (1976) ("the proper standard of materiality must reflect our overriding concern with the justice of the *finding of guilt*") (emphasis added).

The Supreme Court ruling in Brady does not require the prosecutor "to deliver his entire file to defense counsel, but only to disclose evidence favorable to the accused that, if suppressed, would deprive the defendant of a fair trial." See United States v. Bagley, 473 U.S. 667 (1985) (an interpretation of Brady to create a broad, constitutionally required right of discovery 'would entirely alter the character and balance of our present systems of criminal justice'") (citing Giles v. Maryland, 386 U.S. 66, 117 (1967)). An accused's "right to discover [Brady] evidence does not include the unsupervised authority to search through the [government's] files." Ritchie, 480 U.S. at 39. This obligation does not require the United States "to communicate preliminary, challenged, or speculative information." Agurs, 427 U.S. at 110.

The United States has "a duty to learn of any favorable evidence known to the others acting on the government's behalf *in the case*." Kyles, 514 U.S. at 437 (emphasis added). The Court of Appeals for the Armed Forces (CAAF) in Williams outlined the scope of the United States' duty to search for Brady information. See United States v. Williams, 50 M.J. 436, 441 (C.A.A.F. 1999). The Court concluded that the United States must search its own files, the files of law enforcement authorities that participated in the investigation of the subject matter of the charged offense, the investigative files in a related case maintained by an entity closely aligned with the prosecution, and other files, as designated in a defense request, that involve a specified type of information within a specified entity. See id. at 441.

II: THE UNITED STATES HAS PRODUCED ALL DISCOVERABLE INFORMATION THAT IS REQUIRED UNDER RULE FOR COURTS-MARTIAL 703 AND THE CONSTITUTION OF THE UNITED STATES.

In light of the facts and legal authority outlined above, the United States has produced all discoverable information that is required under RCM 703 and the Constitution.

A. The United States produced all discoverable information responsive to Defense request for FOIA materials. See Defense Motion, para. 1(a).

The United States disputes whether the requested information is "relevant and necessary." See R.C.M. 703(f). This information is not relevant to any element of the charged offenses. See R.C.M. 401; see also Article 104, UCMJ; see also Article 134, UCMJ; see also 18 U.S.C. § 641; see also 18 U.S.C. § 793(e); see also 18 U.S.C. 1030(a)(1); see also Article 92, UCMJ. Further, the Defense failed to articulate *any basis* why such information is discoverable. See id. (any defense request "shall include a description of each item sufficient to show its relevance and necessity"). However, on 3 October 2011, the United States produced all enclosures to the CENTCOM FOIA response, specifically BATES 00000772-00000851. See Enclosure 7. The United States intends to produce any remaining portions of the FOIA request, including the actual Reuter's FOIA request, dated 25 July 2007, and any additional documents that were part

of the FOIA response, including the CENTCOM FOIA response, dated 24 April 2009, to the Defense, even though the United States disputes such information is "relevant and necessary." See R.C.M. 703(f)(1).

The United States has not produced all "internal discussions of any such FOIA request." The Defense failed to articulate *any basis* why "internal discussions of any such FOIA request" are "relevant and necessary." The United States bears no obligation to produce such "preliminary, challenged[,] or speculative information." Agurs, 427 U.S. at 110.

B. The United States produced all discoverable information responsive to Defense request for the alleged Quantico video. See Defense Motion, para. 1(b).

The alleged Quantico video does not exist. See Enclosures 2-3. The United States took all reasonable measures to preserve any videos of the alleged incident. See Enclosure 1. LtCol Chris Greer and MSgt Brian Papakie confirmed that all videos were properly provided to the United States. See Enclosures 2-3. On 6 December 2011, the United States produced all such videos to the Defense, specifically BATES 00408902-00408903. See Enclosure 8.

C. The United States has produced all discoverable information responsive to Defense requests for EnCase forensic images of those computers located within the T-SCIF and TOC. See Defense Motion, para. 1(c).

The United States has produced all EnCase forensic images of those hard drives located within the SCIF and TOC that are "relevant and necessary." See R.C.M. 703(f). The United States identified four hard drives within the SCIF that contained the accused's user profile, specifically "bradley.manning," during the deployment. See Enclosures 18-19; see also Enclosures 25-26. On 8 November 2011, the United States produced an EnCase forensic image of all four hard drives with a "bradley.manning" user profile. See Enclosure 20; see also Enclosure 32 (Voucher 073 and Voucher 147-10).

EnCase forensic images of hard drives that do not contain a "bradley.manning" user profile are not "relevant and necessary," thus not discoverable. See R.C.M. 703(f). The Defense argues these forensic images are discoverable "to provide evidence that it was common for [S]oldiers to add technically unauthorized computer programs to their computers." Even assuming, *arguendo*, other Soldiers added unauthorized computer programs, this assumed fact is not relevant to any element of the charged offenses. See R.C.M. 401; see also Article 104, UCMJ; see also Article 134, UCMJ; see also 18 U.S.C. § 641; see also 18 U.S.C. § 793(e); see also 18 U.S.C. 1030(a)(1); see also Article 92, UCMJ. Further, even if relevant, a forensic image of each hard drive is cumulative, thus not necessary. See R.C.M. 703(f)(1) discussion. In the alternative, even if "relevant and necessary," the fact these hard drives were collected from a classified facility, namely the SCIF, confirms that the rules of production under Military Rule of Evidence (M.R.E.) 505 should govern whether these images are discoverable. See M.R.E. 505; see also R.C.M. 703(f) discussion.

The United States took all reasonable measures to preserve any computer located within the SCIF and TOC during the accused's deployment that were relevant to the investigation. See

Enclosures 10-13; see also R.C.M. 703(f)(2) (only "if such evidence is of such central importance to an issue that it is essential to a fair trial, and if there is no adequate substitute for such evidence, the military judge shall grant a continuance or other relief in order to attempt to produce the evidence"). The ARCENT Commander and the FBI confirmed they do not possess any hard drives that were located within the SCIF. See Enclosure 17. The command at 2/10 MTN preserved 181 hard drives, thirteen of which the United States can confirm were located within the SCIF and none of which contained the "bradley.manning" user profile. See Enclosures 14-16. Lastly, CCIU prepared, and the United States produced on 8 November 2011, EnCase forensic images for all hard drives located in the SCIF that contained a "bradley.manning" user profile. See Enclosure 20; see also Enclosure 32 (Voucher 073 and Voucher 147-10).

D. The United States intends to produce discoverable information within the Federal Bureau of Investigations. See Defense Motion, para. 1(b).

The FBI currently has an open law enforcement investigation, which includes some information related to the accused. Based on the information being classified, the United States intends to produce any information within the FBI's investigative files that is discoverable under Brady and directly related to the accused, after the Court issues a protective order for classified information, and based on the United States receiving proper approvals.

E. The Defense has failed to state a legal basis for the production of alleged damage assessments. See Defense Motion, para. 1(d)(1,2,4).

For the reasons that follow, the United States respectfully requests the Court deny Defense's request for damage assessments, if any should exist, from the WTF, IRTF, and DOS.

1. *Background.*

Information may be originally classified only if done so by an original classification authority. Exec. Order No. 13526 § 1.1(a). Additionally, the information must be owned by, produced by or for, or under the control of the United States Government and must fall within one or more of the categories of following categories: military plans, weapons systems, or operations; foreign government information; intelligence activities (including covert action), intelligence sources or methods, or cryptology; foreign relations or foreign activities of the United States, including confidential sources; scientific, technological, or economic matters relating to the national security; United States Government programs for safeguarding nuclear materials or facilities; vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or the development, production, or use of weapons of mass destruction. See Exec. Order No. 13526 §§ 1.1(a), 1.4(a)-(h). Finally, the OCA must determine "that the unauthorized disclosure of the information *reasonably could be expected to result in damage to the national security*" and be able to identify or describe the expected damage. See Executive Order 13526 § 1.1(a) (emphasis added).

OCAs make their classification designations based on their authority under Executive Order 13526, Classified National Security Information (signed by President Barack Obama on

29 December 2009) or for materials classified prior to 27 June 2010 on Executive Order 12958 (signed by President Clinton on 17 April 1995 and amended by Executive Order 13292 signed by President Bush on 25 March 2003), as well as relevant classification guides.

The authority to classify information is limited to (1) the President and the Vice President; (2) agency heads and officials designated by the President; and (3) United States Government officials delegated this authority pursuant to paragraph (c) of section 1.3(a). Executive Order 13526 § 1.3(a).

The President delegated the authority to make classification determinations to heads of selection agencies and it remains an Executive function. Department of Navy v. Egan, 484 U.S. 518, 527 (1988) ("The authority to protect [classified] information falls on the President as head of the Executive Branch and as Commander in Chief."). The authority has been held in the relevant agencies because they have the expertise to review the information and determine the potential impact the release of that information would have on the United States as well as who can have access to that information. Id.; see, e.g., CIA v. Sims, 471 U.S. 159, 176 (1985) ("[A] court's decision whether an intelligence source will be harmed if his identity is revealed will often require complex political, historical, and psychological judgments. . . . There is no reason for a potential intelligence source, whose welfare and safety may be at stake, to have great confidence in the ability of the judges to make those judgments correctly.").

Once an OCA has made a classification determination it is presumed proper and it is not the province of the court to question these determinations. See United States v. Smith, 750 F.2d 1215, 1217 (4th Cir. 1984) ("[T]he government . . . may determine what information is classified. A defendant cannot challenge this classification. A court cannot question it."), vacated and remanded on other grounds, 780 F.2d 1102 (4th Cir. 1985); see also United States v. Rosen, 487 F. Supp. 2d 703, 717 (E.D. Va. 2007) ("Of course, classification decisions are for the Executive Branch . . . ."). The decision of owner of the information must be given great deference. See Sims, 471 U.S. at 176 ("The decisions of the Director, who must of course be familiar with 'the whole picture,' as judges are not, are worthy of great deference given the magnitude of the national security interests and potential risks at stake"); see also Haig v. Agee, 453 U.S. 280, 291 (1981) ("Matters intimately related to foreign policy and national security are rarely proper subjects for judicial intervention"); see also Harisiades v. Shaughnessy, 342 U.S. 580 (1952) (such matters "are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference").

2. *WikiLeaks Task Force.*

The United States has not produced the alleged damage assessment by the WTF because the Defense has failed to provide an adequate basis for its request. See Defense Motion, para. 1(d)(1). The Defense failed to articulate how such information is "relevant and necessary." See R.C.M. 703(f). The Defense merely speculates that an alleged assessment may be "at odds" with a classification review. See Ritchie, 480 U.S. at 59 (the accused "has no constitutional right to conduct his own search of the [government's] files to argue relevance"). This argument confuses the issues – classification reviews are prospective (i.e., "could damage occur"), whereas damage

assessments are in hindsight (i.e., "did damage occur"). Additionally, Defense has not provided any evidence that any OCA had any involvement with the WTF damage assessment.

The alleged damage assessment by the WTF is not "relevant and necessary." R.C.M. 703(f). Actual damage, if any, is not relevant to any element of the charged offenses. See R.C.M. 401; see also Article 104, Uniform Code of Military Justice (UCMJ); see also Article 134, UCMJ; see also 18 U.S.C. § 641; see also 18 U.S.C. § 793(e); see also 18 U.S.C. 1030(a)(1); see also Article 92, UCMJ. The United States need only prove that the compromised information was classified; for example, if "SECRET", that the information "reasonably could be expected to cause serious damage to the national security." See Exec. Order No. 13526. Further, courts consistently reject Defense's proffered relevance of this information. See Smith, 750 F.2d at 1217 (a defendant cannot challenge this classification [determination]"); see also Sims, 471 U.S. at 176 ("The decisions of the Director, who must of course be familiar with 'the whole picture,' as judges are not, are worthy of great deference given the magnitude of the national security interests and potential risks at stake"). Therefore, such information is not "relevant and necessary." R.C.M. 703(f).

3. *Information Review Task Force.*

The United States has not produced the alleged damage assessment by the IRTF because the Defense has failed to provide an adequate basis for its request. See Defense Motion, para. 1(d)(2). The Defense failed to articulate how such information is "relevant and necessary." See R.C.M. 703(f). The Defense merely speculates that an alleged assessment may "undercut the testimony of [] the Original Classification Authority for the charged documents." See Ritchie, 480 U.S. at 59 (the accused "has no constitutional right to conduct his own search of the [government's] files to argue relevance"). This argument confuses the issues – classification reviews are prospective (i.e., "could damage occur"), whereas damage assessments are in hindsight (i.e., "did damage occur"). Additionally, Defense has not provided any evidence that any OCA had any involvement with the IRTF damage assessment.

The alleged damage assessment by the IRTF is not "relevant and necessary." R.C.M. 703(f). Actual damage, if any, is not relevant to any element of the charged offenses. See R.C.M. 401; see also Article 104, Uniform Code of Military Justice (UCMJ); see also Article 134, UCMJ; see also 18 U.S.C. § 641; see also 18 U.S.C. § 793(e); see also 18 U.S.C. 1030(a)(1); see also Article 92, UCMJ. The United States need only prove that the compromised information was classified; for example, if "SECRET", that the information "reasonably could be expected to cause serious damage to the national security." See Executive Order 13526. Further, courts consistently reject Defense's proffered relevance of this information. See Smith, 750 F.2d at 1217 (a defendant cannot challenge this classification [determination]"); see also Sims, 471 U.S. at 176 ("The decisions of the Director, who must of course be familiar with 'the whole picture,' as judges are not, are worthy of great deference given the magnitude of the national security interests and potential risks at stake"). Therefore, such information is not "relevant and necessary." R.C.M. 703(f).

4. *Department of State.*

The DOS has not completed a damage assessment.

5. *Office of the National Counterintelligence Executive.*

The ONCIX has not completed a damage assessment.

F. The Defense has failed both to put the United States on notice of exactly what the Defense desires and to state a legal basis for its production of records from closely aligned investigations. See Defense Motion, para. 1(d)(1-4).

The United States responds as follows to the Defense request for "records from closely aligned investigations." Defense Motion, para. 1(d).

1. *WikiLeaks Task Force.*[3]

The United States denies the Defense request for "any report completed by the WTF" for two reasons. See Defense Motion, para. 1(d)(1). First, the Defense failed to provide an adequate basis in its request, namely what information they seek and how such information is "relevant and necessary." See R.C.M. 703(f). The Defense argues that it is "entitled to receive *all* forensic results and investigative reports by *any* of the cooperating agencies in this investigation" (emphasis added). The United States is not aware of any authority that identifies all reports by all so-called cooperating agencies as relevant and necessary *per se*. Second, the Defense failed to provide specificity in its request. The Defense's request for "[a]ny report completed by the WTF" is *identical* to its request on 13 October 2011. See Enclosure 29. On 27 January 2012, the United States requested "more specificity and an adequate basis for its request." See Defense Enclosure M to its Motion. The Defense again failed to provide any specificity. Requesting "any report completed by the WTF" does not put the United States on notice of exactly what it desires. See Agurs, 427 U.S. at 106 (a request is specific when "it gives the prosecutor notice of exactly what the defense desires"). The United States is unaware of any "forensic results and investigative reports" from within WTF that contributed to any law enforcement investigation.

2. *Information Review Task Force.*

The United States denies the Defense request for "any report generated by the IRTF" for two reasons. See Defense Motion, para. 1(d)(2). First, the Defense failed to provide an adequate basis in its request, namely what information they seek and how such information is "relevant and necessary." See R.C.M. 703(f). The Defense argues that it is "entitled to receive *all* forensic results and investigative reports by *any* of the cooperating agencies in this investigation" (emphasis added). The United States is not aware of any authority that identifies all reports by all so-called cooperating agencies as relevant and necessary *per se*. Second, the Defense failed

[3] Although the WTF is a subordinate organization of the Central Intelligence Agency, the United States separated the defense request for information from both, based on defense's formatting of their request.

to provide specificity in its request. The Defense's request for "any report generated by the IRTF" is hardly more specific than its prior request for "[a]ll forensic results and investigative reports by the Department of Defense," particularly in light of the Defense's knowledge that the IRTF "review[ed] all items allegedly disclosed to WikiLeaks" on behalf of DOD, but outside of law enforcement. See Enclosure 30. On 27 January 2012, the United States requested "more specificity and an adequate basis for its request." See Defense Enclosure M to its Motion. The Defense again failed to provide any specificity. Requesting "any report generated by the IRTF" does not put the United States on notice of exactly what it desires. See Agurs, 427 U.S. at 106 (a request is specific when "it gives the prosecutor notice of exactly what the defense desires"). The United States is unaware of any "forensic results and investigative reports" from within the IRTF that contributed to any law enforcement investigation.

3. *Department of State.*

The United States denies the Defense request for "[a]ll forensic and investigative reports by...DOS" for two reasons. See Defense Motion, para. 1(d)(2). First, the Defense failed to provide an adequate basis in its request, namely how such information is "relevant and necessary." See R.C.M. 703(f). The Defense argues that it is "entitled to receive *all* forensic results and investigative reports by *any* of the cooperating agencies in this investigation" (emphasis added). The United States is not aware of any authority that identifies all reports by all so-called cooperating agencies as relevant and necessary *per se*. Second, the Defense failed to provide specificity in its request. The Defense's request for "[a]ll forensic and investigative reports by...DOS" is *identical* to its request on 8 December 2010. See Enclosure 30. On 27 January 2012, the United States noted that it has produced reports that are "relevant and necessary" to the request, specifically BATES 00408089-00408156 and 00376903 (documents pertaining to the joint investigation between the Diplomatic Security Services (DSS) and CID), but sought "more specificity and an adequate basis" for further discovery. See Defense Enclosure M of its Motion (emphasis added). The Defense again failed to provide any specificity. Requesting "[a]ll forensic and investigative reports by...DOS" does not put the United States on notice of exactly what it desires. See Agurs, 427 U.S. at 106 (a request is specific when "it gives the prosecutor notice of exactly what the defense desires"). Absent the DSS records previously referenced, the United States is unaware of any "forensic results and investigative reports" from within the DOS that contributed to any law enforcement investigation.

In addition to those reasons provided above, the United States denies the Defense request for "any report or assessment by the DOS concerning the released diplomatic cables" for two reasons. See Defense Motion, para. 1(d)(4); see also Prosecution's Response to Defense Motion, para. II (D)(4). First, the Defense failed to provide an adequate basis in its request, namely how such information is "relevant and necessary." See R.C.M. 703(f). The Defense argues that it is "entitled to receive *all* forensic results and investigative reports by *any* of the cooperating agencies in this investigation" (emphasis added). The United States is not aware of any authority that identifies all reports by all so-called cooperating agencies as relevant and necessary *per se*. Second, the Defense failed to provide specificity in its request. The Defense's request for "any report or assessment by the DOS concerning the released diplomatic cables" is hardly more specific than its prior request for "all forensic results and investigative reports by the DOS

regarding the information obtained by WikiLeaks." See Enclosure 30. On 27 January 2012, the United States noted that it has produced reports that are "relevant and necessary" to the request, specifically BATES 00408089-00408156 and 00376903, but sought "more specificity and an adequate basis" for further discovery. See Defense Enclosure M of its Motion. The Defense again failed to provide any specificity. Requesting "any report or assessment by the DOS concerning the released diplomatic cables" does not put the United States on notice of exactly what it desires. See Agurs, 427 U.S. at 106 (a request is specific when "it gives the prosecutor notice of exactly what the defense desires").

4. *Defense Intelligence Agency (DIA).*

The United States denies the Defense request for "[a]ll forensic and investigative reports by...DIA" for two reasons. See Defense Motion, para. 1(d)(2). First, the Defense failed to provide an adequate basis in its request, namely how such information is "relevant and necessary." See R.C.M. 703(f). The Defense argues that it is "entitled to receive *all* forensic results and investigative reports by *any* of the cooperating agencies in this investigation" (emphasis added). The United States is not aware of any authority that identifies all reports by all so-called cooperating agencies as relevant and necessary *per se*. Second, the Defense failed to provide specificity in its request. The Defense's request for "[a]ll forensic and investigative reports by...DIA" is hardly more specific than its prior request for "any and all documents...and reports...conducted by the DIA." See Enclosure 31. On 27 January 2012, the United States requested "more specificity and an adequate basis for its request." See Defense Enclosure M of its Motion. The Defense again failed to provide any specificity. Requesting "[a]ll forensic and investigative reports by...DIA" does not put the United States on notice of exactly what it desires. See Agurs, 427 U.S. at 106 (a request is specific when "it gives the prosecutor notice of exactly what the defense desires"). The United States is unaware of any "forensic results and investigative reports" from within the DIA, including the IRTF, that contributed to any law enforcement investigation.

5. *Office of National Counterintelligence Executive.*

The United States denies the Defense request for "[a]ll forensic and investigative reports by...the ONCIX" for two reasons. See Defense Motion, para. 1(d)(2). First, the Defense failed to provide an adequate basis in its request, namely how such information is "relevant and necessary." See R.C.M. 703(f). The Defense argues that it is "entitled to receive *all* forensic results and investigative reports by *any* of the cooperating agencies in this investigation" (emphasis added). The United States is not aware of any authority that identifies all reports by all so-called cooperating agencies as relevant and necessary *per se*. Second, the Defense failed to provide specificity in its request. The Defense's request for "[a]ll forensic and investigative reports by...ONCIX" is hardly more specific than its prior request for "any damage assessment or review completed in this case either by or with the assistance of ONCIX." See Enclosure 4. On 27 January 2012, the United States requested "more specificity and an adequate basis for its request." See Defense Enclosure M of its Motion. The Defense again failed to provide any specificity. Requesting "[a]ll forensic and investigative reports by...ONCIX" does not put the United States on notice of exactly what it desires. See Agurs, 427 U.S. at 106 (a request is specific when "it gives the prosecutor notice of exactly what the defense desires"). The United

States is unaware of any "forensic results and investigative reports" from within the ONCIX that contributed to any law enforcement investigation.

6. *Central Intelligence Agency.*

The United States denies the Defense request for "[a]ll forensic and investigative reports by...CIA" for two reasons. See Defense Motion, para. 1(d)(2). First, the Defense failed to provide an adequate basis in its request, namely how such information is "relevant and necessary." See R.C.M. 703(f). The Defense argues that it is "entitled to receive all forensic results and investigative reports by any of the cooperating agencies in this investigation" (emphasis added). The United States is not aware of any authority that identifies all reports by all so-called cooperating agencies as relevant and necessary per se. Second, the Defense failed to provide specificity in its request. The Defense's request for "[a]ll forensic and investigative reports by...CIA" is hardly more specific than its prior request for "any and all documentation related to the CIA investigation of WikiLeaks." See Enclosure 30. On 27 January 2012, the United States requested "more specificity and an adequate basis for its request." See Defense Enclosure M of its Motion. The Defense again failed to provide any specificity. Requesting "[a]ll forensic and investigative reports by...CIA" does not put the United States on notice of exactly what it desires. See Agurs, 427 U.S. at 106 (a request is specific when "it gives the prosecutor notice of exactly what the defense desires"). The United States is unaware of any "forensic results and investigative reports" from within the CIA that contributed to any law enforcement investigation.

7. *Department of Justice.*

On 20 September 2011, the United States produced information "relevant and necessary" to Defense's request for "any information relating to any 18 U.S.C. § 2703(d) order or any search warrant by the government of Twitter, Facebook, Google or any other social media site[,]" specifically BATES 00022960-00023077, 00023607-00023623, 00036691-00036722. See Enclosure 7; see also Defense Motion, para. 1(d)(3); see also R.C.M. 703(f). The United States is in the process of producing all discovered information "relevant and necessary" to Defense's request that the United States has authority to disclose under the federal rules. The United States disputes whether Defense provided a specific request, and adequate basis, for its request for "any grand jury testimony." See Defense Motion, para. 1(d)(3). However, in an abundance of caution, the United States intends to produce all grand jury materials, both classified and unclassified, that are "relevant and necessary" and that the United States has authority to disclose under the federal rules. See R.C.M. 703(f)(1). Absent the FBI law enforcement files previously referenced, the United States is unaware of any "forensic results and investigative reports" from within the DOS that contributed to any law enforcement investigation.

CONCLUSION

Based on the above, the United States respectfully request the Court deny Defense request to compel the production of the following: (1) internal discussion of any FOIA request; (2) EnCase forensic images of all preserved hard drives that do not contain the

"bradley.manning" user profile; (3) and damage assessments and records from the Central Intelligence Agency (CIA), Department of Defense (DOD) (including all agencies or departments referenced in Defense Motion, para. 1(d)(2)), Department of Justice (DOJ), and Department of State (DOS).

ASHDEN FEIN
CPT, JA
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel and Major Matthew Kemkes, Senior Military Defense Counsel, via electronic mail, on 8 March 2012.

ASHDEN FEIN
CPT, JA
Trial Counsel